DEA Diversion Control E-Commerce System

Certificate Policy

Version 2.0

Prepared for

Drug Enforcement Administration
E-Commerce Program (ODC)
Washington, D.C. 20537

April 29, 2005

Prepared by
PEC Solutions Inc.

Signature Page

Chair, DEA Diversion Control E-Commerce System PMA **DATE**

Table of Contents

Page

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Section 1 – Introduction

The Drug Enforcement Administration (DEA) regulates the manufacture, distribution and dispensing of controlled substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and also to ensure that there is a sufficient supply for legitimate medical uses. The DEA presently operates two programs under the DEA Diversion Control E-Commerce System Bridge Certification Authority (referred to as the "DEA Bridge CA" in this document), the Electronic Prescriptions for Controlled Substances (EPCS) and the Controlled Substance Ordering System (CSOS).

The EPCS program allows the electronic transfer of controlled substance prescriptions between practitioners and pharmacies using Public Key Infrastructure (PKI) technology to digitally sign the electronic transaction. The electronic transmission of Schedules II – V prescriptions for controlled substances by EPCS participants shall only be authorized by DEA provided the Subscriber demonstrates acceptance of the applicable provisions of this Certificate Policy (CP) and the prescription form is digitally signed using the digital certificate issued to the practitioner by a DEA-approved CA.

Within the EPCS program, the DEA does not issue digital certificates directly to Subscribers, but issues certificates only to Certification Authorities (CAs) approved by the DEA who, in turn, provide EPCS digital certificates to authorized Subscribers. EPCS supports interoperability of Federal agency PKI domains and allows CAs approved by the DEA Diversion Control E-Commerce System Policy Management Authority (PMA) to participate as EPCS CAs. Subscriber certificates issued under EPCS must be consistent with the DEA Diversion Control E-Commerce System Certificate and CRL Profile and must identify the individual named in the certificate, bind that person to a particular public/private key pair, and provide sufficient information demonstrating the Subscriber is operating under the authority of the DEA EPCS program. Subscribers must demonstrate acceptance of the DEA Diversion Control E-Commerce System CP by signing a Subscriber Agreement

Qualification of applicant EPCS CAs is dependent on their proven compliance with this CP, development of an approved Certification Practices Statement (CPS), and either the ultimate incorporation of the subordinate CA under, or successful cross-certification with, the DEA Bridge CA trust hierarchy. Throughout this document, the term "CA" shall be used when referencing provisions applicable to all Certificate Authorities, while provisions affecting only the DEA Bridge CA or subordinate and cross-certified CAs shall be so designated.

DEA's CSOS program allows the electronic ordering of controlled substances between controlled substance manufacturers, distributors, pharmacies, and other DEA authorized

ordering entities, using PKI technology to digitally sign the electronic transactions. The CSOS CA serves as the central element responsible for establishing a trust relationship between these trading partners, instituting the security services of authenticity, integrity and non-repudiation into the DEA's controlled substance electronic ordering system.

The CSOS CA shall be operated under the authority of the DEA Office of Diversion Control PMA as a subordinate CA to the DEA Bridge CA. CSOS end entity (Subscriber) certificates are issued only by the CSOS CA. These Subscriber certificates identify the individual named in the certificate, bind that person to a particular public/private key pair, and provide sufficient information demonstrating that the Subscriber is operating under the authority of the DEA CSOS program. Subscribers must demonstrate acceptance of the DEA Diversion Control E-Commerce System CP by signing a Subscriber Agreement

The *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document, produced under separate cover, provides the necessary guidance for certificate profiles within the DEA Diversion Control E-Commerce System.

This DEA Diversion Control E-Commerce System CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, *Certificate Policy and Certification Practice Statement Framework*.

The terms and provisions of this CP shall be interpreted under and governed by applicable Federal and State Law. The United States Government disclaims any liability that may arise from the use of this CP.

1.1 Overview

A Certificate Policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [X.509].

This document, along with the *Certificate and CRL Profile* document, defines the creation and management of certificates for use in both electronic prescription and electronic ordering applications for controlled substances. This document establishes the level of assurance and trust that can be placed in the authenticity and integrity of the public keys contained in certificates issued by authorized CAs. The word "assurance" used in this CP indicates to what extent a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. The associated EPCS CPS and CSOS CPS describe the practices of the DEA Diversion Control E-Commerce System and its CAs. It shall be used to establish the level of assurance and trust that can be placed in the authenticity and integrity of the public keys contained in certificates that are issued by the DEA Bridge CA. This CP specifies

(1) the Certification Authorities, the Subscribers, and the Relying Parties authorized to participate in the PKI program described by this policy, (2) the obligations of the participants governed by this CP, and (3) the minimum requirements for the issuance and management of digital certificates used in verifying transactions and digital signatures in EPCS and CSOS applications.

1.2 Identification

This CP addresses EPCS and CSOS certificates that are defined in subsequent sections of this document. This CP is registered with the National Institute of Standards and Technology (NIST) and has been assigned the following object identifiers (OIDs) for the DEA Diversion Control E-Commerce System certificates defined in this policy.

CSOS Certificates: dea-csos-cp ::= { 2.16.840.1.101.3.2.1.9.1}

EPCS Certificates: dea-epcs-cp ::= { 2.16.840.1.101.3.2.1.9.2 }.

All EPCS and CSOS certificates issued under this policy by subordinate CAs shall reference this policy by including the appropriate OID for this policy in the Certificate Policies field of the EPCS or CSOS Certificate. The foregoing OIDs may not be used except as specifically authorized by this policy.

Cross-certified EPCS CAs shall, in the *policyMappings* extension and in whatever other fashion is defined by the PMA to be necessary for interoperability, reflect what mappings the PMA determines shall exist between this CP and the affected Entity CP. All EPCS CA certificates issued by the DEA CA shall include basic constraints with a path length constraint set to zero, establishing the DEA Bridge CA as its "trust anchor".

1.3 Community and Applicability

The following sections discuss the roles relevant to the administration and operation of the DEA Diversion Control E-Commerce System.

1.3.1 PKI Authorities

1.3.1.1 DEA Diversion Control E-Commerce System Policy Management Authority (PMA)

The DEA Diversion Control E-Commerce System PMA has been tasked by the Office of Diversion Control (OD) to be the governing body responsible for the DEA Diversion Control PKI initiative. PMA membership consists of selected individuals working within the DEA Office of Diversion Control, E-Commerce Section (ODC), Liaison and Policy Section (ODL), Registration and Program Support section (ODR), the DEA Diversion

Control PKI Operations Management Authority (OMA), the DEA CIO or his or her representative and the Contracting Officer's Technical Representative (COTR) supervising contractor activities relating to the DEA Diversion Control E-Commerce System.

The mission of the DEA Diversion Control E-Commerce System PMA is to establish, interpret, and enforce policy for the CSOS and EPCS PKI initiatives in accordance with all applicable U.S. laws and regulations. Additional responsibilities include:

- Approving the DEA Diversion Control E-Commerce System CP;
- Approving the CSOS CPS;
- Approving the EPCS CPS;
- Accepting applications from parties desiring to participate as a EPCS CA;
- Approving the CP and/or CPS submitted by EPCS CA applicants;
- Ensure conformance to applicable requirements as a condition for allowing continued interoperability with EPCS.

1.3.1.2 DEA Diversion Control E-Commerce System Operations Management Authority (OMA)

The Operations Management Authority, or OMA, reports to the PMA and is responsible for the daily operation and maintenance of the DEA Electronic Commerce PKI systems. The OMA also provides planning guidance and directs the activities of the DEA Electronic Commerce PKI Manager and the PKI manager's staff.

1.3.1.3 DEA Diversion Control E-Commerce System Bridge Certification Authority (DEA Bridge CA)

The DEA Bridge CA shall be established by the DEA. It shall be operated and maintained by the DEA or by an authorized DEA contractor. The DEA Bridge CA shall operate in accordance with the provisions of its Certification Practices Statement. The DEA Bridge CA shall perform the following functions:

- Issue and manage certificates to entities authorized as EPCS subordinate Certificate Authorities approved by the PMA, as defined in this CP;

- Issue and manage cross-certification certificates as approved by the PMA, this includes those issued to authorized EPCS CAs, as defined in this CP, or other external CAs, such as the Federal Bridge CA;

- Issue and manage the CSOS Subordinate Certification Authority approved by the PMA, as defined in this CP; and

- Publish subordinate and cross-certified CA certificate status information.

1.3.1.4 Authorized EPCS Certification Authorities (EPCS CA)

An EPCS CA is an entity authorized by the PMA to create, sign, and issue public key certificates to authorized EPCS Subscribers, either through subordination to the DEA Diversion Control E-Commerce Bridge CA (referred to as the DEA Bridge CA) or through the granting of a unilateral cross-certificate. The EPCS CA is responsible for all aspects of the issuance and management of a certificate, including: the registration process, the identification and authentication process, the certificate manufacturing process, the revocation of certificates, and for ensuring that all aspects of the CA services and CA operations and infrastructure related to the certificates issued under the *DEA Diversion Control E-Commerce System Certificate Policy* are performed in accordance with the requirements, representations, and warranties of this CP. EPCS CAs shall conform to the stipulations of this CP definition and publish a CPS that supports and includes references to this CP, while cross-certified CAs must demonstrate compliance through a policy mapping of the entity's CP and examination of their CPS.

1.3.1.5 CSOS Subordinate Certification Authority (CSOS CA)

The CSOS CA is an entity established and authorized by the PMA to create, sign, and issue public key certificates to authorized CSOS Subscribers through subordination to the DEA Diversion Control E-Commerce Bridge CA. It shall be operated and maintained by the DEA or by an authorized DEA contractor. The CSOS CA is responsible for all aspects of the issuance and management of a certificate, including: the registration process, the identification and authentication process, the certificate manufacturing process, the revocation of certificates, and for ensuring that all aspects of the CA services and CA operations and infrastructure related to the certificates issued under the *DEA Diversion Control E-Commerce System Certificate Policy* are performed in accordance with the requirements, representations, and warranties of this CP. The CSOS CA shall conform to the stipulations of this CP definition and publish a CPS that supports and includes references to this CP.

1.3.1.6 Registration Authorities (RA)

A Registration Authority is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificates. The following entities have been identified as functioning as RAs for the DEA Diversion Control E-Commerce System:

1.3.1.6.1 EPCS CA RA

Each EPCS CA shall perform the role and functions of a RA. These CAs shall process EPCS Subscriber registrations; collecting and verifying Subscriber identity and

information that is to be entered into the Subscriber's public certificate. EPCS CAs shall operate according to the stipulations of this CP. The EPCS CA may employ agents who agree to be bound by this policy, but the EPCS CA remains responsible for the performance of those services in accordance with this policy and the requirements of its CPS.

The DEA Diversion Control E-Commerce System OMA acts as the RA for EPCS CAs seeking subordination or cross-certification to the DEA Bridge and performs its functions in accordance with the procedures specified in the CPS.

1.3.1.6.2 CSOS RA

The CSOS CA shall perform both the role and the functions of a RA. The CSOS RA shall process applications of CSOS Coordinators and Subscribers, verifying the information that is to be entered into the Subscriber's public certificate and shall operate according to the stipulations of this CP. Individuals applying for CSOS Certificates are required to do so through their CSOS Coordinator.

1.3.2 CSOS Coordinator

A DEA Registrant must appoint a CSOS Coordinator who will serve as that Registrant's recognized agent regarding issues pertaining to the issuance of, revocation of, and changes to digital certificates issued under that registrant's DEA registration. These individuals serve as knowledgeable liaisons between one or more DEA registered locations and the CSOS Certification Authority (CA). The coordinators will collect applications, ensure that they include all of the required information, have the package notarized, and send it to the CA.

1.3.2.1 CSOS Principal Coordinator

A CSOS Principal Coordinator may be any individual employed by the organization, however unless otherwise indicated, the person who signed the most recent DEA Registration application shall serve the role of CSOS Principal Coordinator.

1.3.2.2 CSOS Alternate Coordinator

A CSOS Alternate Coordinator shall serve as an organization's secondary CSOS contact for the DEA Registration(s) identified on their application. A CSOS Alternate Coordinator may be any individual employed by the organization. Establishment of a CSOS Alternate Coordinator is optional.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate issued by an authorized DEA Diversion Control E-Commerce System CA, who attests that it uses its key and certificate in accordance with the CP asserted in the certificate. The DEA Diversion Control E-Commerce System includes the following types of Subscribers:

1.3.3.1 EPCS Subscribers

EPCS Subscribers are limited to DEA registrants and agents of registrants as stipulated in DEA's regulations. DEA allows practitioners who are agents of a registered institutional practitioner to use the registrant's DEA number to sign prescriptions for controlled substances. The authorizing institution must assign an internal authorization code assigned to each agent. This internal code takes the form of a suffix to the authorizing institution's DEA number and the authorizing institution must keep a record of these internal codes.

1.3.3.2 CSOS Subscribers

CSOS Subscribers are limited to approved DEA Registrants and those individuals that hold Power of Attorney (POA) for DEA Registrants.

1.3.4 Relying Parties

A Relying Party is the entity that, by using a Subscriber's certificate to verify the integrity of a digitally signed message, identifies the creator of a message, and relies on the validity of the public key bound to the Subscriber's name. The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party uses the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

1.4 Applicability

EPCS Subscriber certificates shall only be issued to individuals with controlled substance prescribing authority and must be used for the signing of electronically transmitted controlled substance prescriptions or the signing of electronic orders, however the use of EPCS certificates is not restricted to this single application. EPCS certificates are appropriate for use with other applications requiring a High level of assurance or below, as defined by the FBCA. This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

CSOS Subscriber certificates shall only be issued to entities engaged in the transfer of controlled substances between manufacturers, distributors, retail pharmacies, authorizing institutions and other registrants and must be used for the signing of electronic transaction orders, however the use of CSOS certificates is not restricted to this single application. While EPCS Subscriber certificates may be used to sign electronically transmitted orders, CSOS certificates may not be used for the signing of electronically transmitted controlled substance prescriptions. CSOS certificates are appropriate for use with other applications requiring a Medium level of assurance or below, as defined by the FBCA. This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

1.5 Contact Details

1.5.1 Specification Administration Organization

The DEA Diversion Control E-Commerce System PMA has been tasked by the Office of Diversion Control (OD) to be the governing body responsible for the DEA Diversion Control PKI initiative and all aspects of this CP.

1.5.2 Contact Person

Direct all questions regarding this CP, Version 2.0 dated December 15, 2004, to the Chair of the Policy Management Authority, whose contact information can be found at http://www.DEAecom.gov. Written communications may be sent to the following address:

Drug Enforcement Administration
E-Commerce Program (ODC)
Attn: Chair, Policy Management Authority
Washington, DC 20537

1.5.3 Person Determining CPS Suitability for the Policy

The DEA Diversion Control E-Commerce System PMA shall approve any CPS of the DEA Bridge and subordinate or cross-certified EPCS CAs. The Bridge, subordinate and cross-certified CAs shall be required to attest to the compliance of their CPS periodically as set forth in this CP.

Section 2 — General Provisions

This section specifies any applicable presumptions on a range of legal and general practice topics.

2.1 Obligations

2.1.1 PMA Obligations

The PMA is responsible for providing oversight of the DEA Diversion Control E-Commerce System program, reviewing and approving the Certificate Policy, Certification Practices Statement, and Subscriber Agreements. Additionally, the PMA will

- Resolve any name claim disputes;
- Approve any fees levied by the OMA;
- Establish the qualifications for the selection of entities seeking to perform a compliance audit;
- Review compliance audits and make appropriate determinations; and
- Ensure that CSA database information is readily available for verification.

2.1.2 OMA Obligations

The OMA is responsible for daily operations of the DEA Diversion Control E-Commerce System, ensuring that operations adhere to the policies and practices defined in this CP and the CPS.

2.1.3 CA Obligations

2.1.3.1 DEA Diversion Control E-Commerce System Bridge CA Obligations

The DEA Bridge CA shall conform to the stipulations of this document including:

- Protect the private signing key of the DEA Bridge CA in accordance with this CP;

- Sign certificates only after verifying the identity of the certificate subject in accordance with this CP, and that the subject holds the private key corresponding to the public key in the certificate;
- Use the private signing key only when issuing certificates or signing Authority Revocation Lists (ARLs) which conform to this CP;
- Provide to the PMA a CPS, as well as any subsequent changes, for conformance assessment;
- Conform to the stipulations of the approved CPS;
- Operate or provide for the service of a repository for maintaining CA certificate information and status;
- Revoke the certificates of CAs found to have acted in a manner counter to those obligations it agreed to conform and attest to;
- Provide for certificate updating or re-keying.

2.1.3.2 CA Obligations

A CA that issues EPCS or CSOS Subscriber certificates shall conform to the stipulations of this document, including:

- Provide a CPS to the PMA, as well as any subsequent changes to the CPS, for conformance assessment;
- Conform to the stipulations of the approved CPS;
- Protect the CA's private signing key in accordance with this CP;
- Sign certificates only after verifying the identity of the certificate subject in accordance with this CP, and that the subject holds the private key corresponding to the public key in the certificate;
- Use the private signing key only when issuing certificates or signing Certificate Revocation Lists (CRL) which conform to this CP;
- Ensure that registration information is accepted only from RAs who understand and are obligated to comply with this CP;
- Include only valid and appropriate information in the certificate, and maintain evidence that due diligence was exercised in validating the information contained in the certificate;

- Ensure that Subscribers are informed of their obligations as defined in this CP, and are informed of the consequences of not complying with those obligations;
- Revoke the certificates of Subscribers found to have acted in a manner counter to those obligations;
- Provide for certificate updating or re-keying;
- Operate or provide for the service of a repository for maintaining Subscriber certificate information and status;
- Maintain records necessary to support requests concerning its operation, including audit files and archives.
- Accurately publish CRLs, process certificate applications and respond to revocation requests in a timely and secure manner in accordance with this CP;

A CA that is found to have acted in a manner inconsistent with these obligations is subject to action as described within this CP.

2.1.4 RA Obligations

2.1.4.1 EPCS RA Obligations

EPCS CAs shall be responsible for performing Subscriber identification and authentication functions, and agree to be bound by the terms of this CP. The CA may delegate specific activities supporting these functions to identified Registration Authorities provided that the CA remains responsible for the services provided by these agents and warrants that these activities shall be conducted in accordance with this CP.

The DEA Diversion Control E-Commerce System OMA shall serve as the RA for approved EPCS CAs seeking cross-certification or subordination to the DEA Bridge, in accordance with procedures specified in the EPCS CPS.

2.1.4.2 CSOS RA Obligations

The CSOS RA is responsible for controlling the registration process through the adjudication of applications received from CSOS Coordinators and Subscribers, collecting and verifying the information to be entered into the certificates issued by the CSOS CA. DEA has chosen to delegate some of the RA activities to designated CSOS Coordinators as specified below.

2.1.4.2.1 CSOS Coordinator Obligations

CSOS Coordinators (Principal Coordinators and Alternate Coordinators) serve as Local Registration Authorities (LRAs). For individuals applying for a CSOS certificate associated with a DEA registered location for which the CSOS Coordinator is responsible, the CSOS Coordinator shall:

- Verify the applicant's identity and employment;
- Verify that the applicant's CSOS application packet has been properly completed and signed by the applicant;
- Sign and submit the completed application packet to the CSOS Registration Authority;
- Maintain evidence that due diligence was exercised in validating the information contained in the Subscriber's application;
- Serve as a point of contact for CSOS notification for their registered location, supplying confirmation of certificate requests, certificate re-keying or updates, and revocation requests.

2.1.5 Subscriber Obligations

In all cases, prior to releasing or publishing an EPCS or CSOS certificate, the CA shall ensure that the Subscriber named in the certificate has signed a Subscriber Agreement agreeing to be bound by this CP as a Subscriber and obligating the Subscriber to:

- Protect their private key in accordance with this CP and as stipulated in their certificate acceptance agreement, taking all reasonable measures to prevent its loss, disclosure, modification, or unauthorized use;

- Acknowledge that by accepting the certificate, the Subscriber is warranting that all information and representations made by the Subscriber included in the certificate are true;

- Use the certificate only for authorized and legal purposes, consistent with this CP;

- Notify the issuing CA in accordance this CP if they suspect that their private key is compromised or lost;

- Abide by all terms, conditions, and restrictions levied upon the use of their private keys and certificates.

2.1.6 Relying Party Obligations

Relying parties are responsible for performing checks for validity of each digitally signed prescription as required by applicable federal and state regulations. Relying parties are responsible for examining the CP to understand all of their rights and obligations under the CP.

2.1.7 Repository Obligations

Each CA shall ensure that there is a repository where the DEA Bridge CA certificate and revocation lists are published and available for status checking. CSOS and EPCS Subscriber certificates shall not be made publicly available. The repository shall be an X.500 compliant directory with the Lightweight Directory Access Protocol (LDAP) access. The CA shall assert a high level of reliability and availability of the repository. ARLs and CRLs must be published in accordance with this CP. The DEA Bridge CA shall publish this CP on DEA's web site at http://www.DEAecom.gov. All CAs shall make this CP publicly available either in an online repository or a web site that is available to Subscribers and Relying Parties.

2.2 Liability

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Parties

The PMA, DEA Bridge CA, and CSOS CA assume no financial responsibility for improperly used certificates.

2.3.2 Fiduciary Relationships

Issuance of certificates in accordance with this CP shall not make the DEA Bridge CA an agent, fiduciary, trustee, or other representative of the subordinate or cross-certified CAs or their Subscribers.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The laws of the United States of America and the laws of the states in which the Subscriber and Relying Party are domiciled shall govern the enforceability, construction, interpretation, and validity of this CP.

2.4.2 Severability, Survival, Merger, Notice

Should it be determined that one section of this CP is incorrect or invalid, the other sections shall remain in effect until the policy is updated. Requirements for updating this CP are described in Section 8.

2.4.3 Dispute Resolution Procedures

Every attempt should be made to resolve the dispute by negotiation, however the PMA shall have the sole authority for the resolution of any disputes by quorum vote of the membership. CAs must describe dispute resolution procedures in their CPS. The PMA shall resolve any dispute arising out of this CP unless precluded by governing law or other agreement. Disputes requiring PMA resolution should be provided in writing to the PMA at the address specified in Section 1.

2.5 Fees

The CAs shall not impose any fees to end entities for the reading of this CP or any other document incorporated by reference. The CA may charge fees for the issuance of certificates as well as access to certificates or certificate status information, subject to agreement between the CA and Subscriber and/or between the CA and Relying Party, and in accordance with a fee schedule publicly published by the CA in its CPS and on its Web site. If fees are charged for certificate issuance or status checking, the CA must clearly post a refund policy on their Web site.

2.6 Publication and Repository

2.6.1 Publication of CA Information

Each CA shall publish the following information to either an online repository or a Web site that is available to Subscribers and relying parties.

- A CRL;
- The CA's certificate;
- A copy of this CP, including any waivers granted to the CA by the PMA.

The CA's certificate and ARLs associated with subordinate CAs shall be made publicly available in the DEA Bridge CA repository.

Subscriber certificates shall not be made publicly available in CSOS or EPCS repositories.

2.6.2 Frequency of Publication

All information to be published in the repository shall be published according to the parameters established within this CP.

2.6.3 Access Controls

The information in the DEA Bridge CA directory shall be publicly available through the Internet. There shall be no access controls on the reading of this CP. CAs shall implement appropriate access controls restricting who can write or modify policies, certificates, certificate status or ARLs/CRLs. Access to Subscriber certificates located in the repositories is restricted to CA personnel. Subscriber certificates shall not be made publicly available in CSOS or EPCS repositories.

2.6.4 Repositories

The location of the repositories shall be appropriate to the certificate-using community and must be specified in the CPS.

2.7 Compliance Audit

Each CA shall have a compliance audit mechanism in place to ensure that the requirements of this CP and their CPS are being implemented and enforced. Compliance audits shall use the American Institute of Certified Public Accountants (AICPA) WebTrust for Certificate Authorities criteria and shall adhere to the scope and report format established by the PMA.

2.7.1 Frequency of Entity Compliance Audit

Certification Authorities shall undergo a compliance audit prior to initial certification as an authorized CA to demonstrate compliance with this CP and their CPS. Re-certification shall be required no less than once per year. The PMA reserves the right to conduct periodic and unscheduled compliance audits or inspections of the DEA Bridge CA and subordinate or cross-certified CAs, RAs or any Local RA services being provided in order to validate that the these entities are operating in accordance with the security practices and procedures described in their respective CPS.

2.7.2 Identity/Qualifications of Auditor

The auditor seeking to perform a compliance audit must be Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices. The auditor must be qualified to perform an AICPA audit and must be thoroughly familiar with the requirements that the PMA defines for the issuance and management of EPCS and CSOS certificates as provided in this CP. The compliance auditor must perform such compliance audits as a primary responsibility.

2.7.3 Auditor's Relationship to Audited Party

The compliance auditor and the CA shall have sufficient organizational independence to ensure an unbiased, independent, and repeatable evaluation.

2.7.4 Topics Covered by Audit

The purpose of the compliance audit shall be to verify that the CA has a system in place to assure that its operational policies and procedures are consistent with the requirements stated in this CP and its CPS.

2.7.5 Actions Taken as a Result of Deficiency

Should the compliance auditor find a discrepancy between a CA's operation and the stipulations in this CP or its CPS, the following must occur:

- The compliance auditor shall note the discrepancy;
- The CA shall provide written notification of the audit results to the PMA, specifically identifying any deficiencies noted as a result of the compliance audit, within 3 business days;
- Once notified, the PMA and OMA shall have 10 business days to review the results and the recommendations from the compliance audit to determine the action to be taken. Several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate-using community

Based on the findings of the compliance audit, appropriate remedies that the PMA may take may include any of the possible following actions:

- Warn the CA in writing and specify a time period during which the discrepancy must be resolved;
- Immediately suspend the CA's authority to issue new certificates;
- Revoke the CA's certificate.

Upon correction of the discrepancy, the CA may request reauthorization. A special audit may be required to confirm the implementation and effectiveness of the remedy.

2.7.6 Communication of Results

If the CA is found to be non-compliant with the CPS or this CP, the PMA may take action as specified in the section above. Required remedies shall be defined and communicated to the CA as soon as possible to limit the risks identified.

2.8 Confidentiality

The results of audits will be kept confidential, with exceptions as deemed appropriate by the PMA.

The CA shall keep all Subscriber information confidential with the exception of information that is included in the certificate. Subscriber information from this system may be disclosed to the following parties:

- To federal, state or local agencies along with state medical and licensing boards responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order when the DEA Office of Diversion Control becomes aware of a violation or potential violation of civil or criminal law or regulation.
- To a member of Congress or to a congressional staff member in response to a request from the person who is the subject of the record.
- To a DEA employee, an expert consultant, or contractor of DEA in the performance of a federal duty to which the information is relevant.
- Persons registered under the Controlled Substances Act (P.L. 91-513) for the purpose of verifying the registration of customers and practitioners.

Unless otherwise required by law and under the conditions stated above, Subscriber information shall be used only for the purpose collected and agreed and such information shall not be released without the prior written consent of the Subscriber. Any request for release of Subscriber information shall be authenticated.

2.9 Intellectual Property Rights

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in the EPCS or CSOS Certificate. This CP and associated OIDs are the exclusive property of U.S. Government. CAs may only use associated OIDs in accordance with the provisions of this CP.

Section 3 — Identification and Authentication

3.1 Initial Registration

3.1.1 EPCS Registration

3.1.1.1 EPCS CA Registration

Subordinate CA applicants, or CAs wishing to cross-certify with EPCS, shall submit a completed application together with their CPS and other requested documentation to the PMA for review. Applicants entering into a binding agreement with the PMA must comply with the following subsections. Information on the application process and required documentation is provided on DEA's web site at http://www.DEAecom.gov.

In the event that the PMA denies a Certification Authority's application to become a participating EPCS CA, the CA whose certificate has been denied may, within thirty calendar days of receipt of notification of the denial, submit written comments or written objections to the denial. The applicant will be provided a written notice citing the legal and factual basis for denial of the application. At the same time, the CA whose certificate has been denied also may provide supporting documentation to contest the denial. If such written comments or written objections raise issues regarding any finding of fact or conclusion of law upon which the denial is based, the DEA Administrator will reconsider the denial in light of the written comments or written objections filed. Within 10 days of receipt of the written comments or written objections, DEA may file a response to such written comments or written objections, which the DEA Administrator will address in making the final decision to maintain or withdraw the denial. Thereafter, within a reasonable time, the DEA Administrator will withdraw or affirm the original denial as he determines appropriate. The DEA Administrator will provide written reasons for any affirmation of the original denial. Such affirmation of the original denial will constitute a final decision for purposes of judicial review under 21 U.S.C. 877.

3.1.1.2 EPCS Subscriber Registration

Issuance of an EPCS Subscriber certificate by an EPCS CA is subject to the CA's approval, acceptance of the applicant's EPCS certificate application, and of good standing in the DEA's Controlled Substances Act (CSA) database.

Subscribers shall enter into a binding agreement with the CA as cited in Section 2.1.5 and submit their application in compliance with the directives in 3.1.11.1. The CA is responsible for obtaining identity verification and authorization of the Subscriber through the DEA's CSA database. EPCS Subscribers shall be DEA registered practitioners or agents of DEA registered institutions (hospitals and clinics) that are listed in the CSA

database and are authorized to write prescriptions for controlled substances. The PMA shall ensure that applicable CSA database information is readily available for verification.

An EPCS CA must establish procedures in its CPS so that if the CA denies a Subscriber's application, the CA must provide written notice of the reasons for denial of the application, an opportunity for the practitioner to submit a written response, and a final written decision by the EPCS CA. The EPCS CA is required to notify DEA of such a denial and provide a copy of all pertinent written materials prior to issuance of the denial when such final denial is based upon DEA-mandated requirements.

3.1.2 CSOS Registration

Separate application processes are established for the identification of DEA Registrants, an organization's CSOS Coordinators and Subscriber applications. CSOS Coordinator and certificate applications and instructions can be found at DEA's Web site at http://www.DEAecom.gov.

3.1.2.1 CSOS Coordinator Registration

A notarized CSOS Coordinator or DEA Registrant application must be received along with or prior to any CSOS POA certificate applications. Registrants and POAs applying as the CSOS Coordinator shall be given the option to receive a CSOS certificate on the CSOS Coordinator application form.

3.1.2.2 CSOS Subscriber Registration

CSOS Subscribers shall be DEA registrants who are listed in the CSA database or holders of a valid power of attorney for those registrants and shall enter into a binding agreement with the CSOS CA.

Subscriber applications are submitted to the CSOS Coordinator. The CSOS Coordinator is responsible for the initial verification of the Subscriber's identity and authorization for a CSOS certificate and submission of the application package to the CSOS RA.

Organizations not utilizing chain renewal require that the registrant, or registrant's POA, submit a duly notarized application packet to the CSOS RA. Upon receipt of the application package, the CSOS RA shall cross reference application data with the DEA's CSA database. The PMA shall ensure that CSA database information is readily available for verification

3.1.2.3 CSOS Subscriber Bulk Enrollment

Bulk Enrollment processes have been established to accommodate organizations that need to obtain a large volume of CSOS Certificates associated with a single applicant, such as chain pharmacies utilizing centralized ordering wherein one individual has been assigned the responsibility of ordering controlled substances for delivery to multiple locations – each order requiring a Subscriber to hold a digital certificate for that DEA Registrant. In order to participate in CSOS Bulk Enrollment, an organization must currently participate in the DEA Chain Renewal program described at http://www.deadiversion.usdoj.gov/drugreg/chain_renewal.htm. This procedure was developed by DEA to simplify the renewal application process for companies that maintain registrations at multiple locations, for example chain pharmacies. The procedure allows corporations to renew all of their DEA registrations at the same time, thereby eliminating the need for multiple applications. This simplified application process is available to corporations with 50 or more retail pharmacy registrations or distributors with 10 or more registered locations. Each applicant (DEA Registrant, Principal Coordinator, Alternate Coordinator, and POA), will complete his/her application as specified in the above processes with the exception of how the DEA Registration and POA documentation is submitted. Enrollment instructions exist on the CSOS Web site at http://www.DEAecom.gov. The CSOS RA will work with the organization's primary point of contact for bulk enrollment to ensure the DEA Registration and POA documentation are submitted correctly.

3.1.3 Types of Names

Names of EPCS and CSOS certificate subjects must be X.500 Distinguished Names (DN). The Common Name (CN) must be the same as the Subscriber's legal name, such as that which Federal or local records use to refer to that person (i.e. POA letter, agent practitioner authorization letter for agent practitioners, human resources documents, birth certificate or driver's license). For registrants, the DN must correspond to the registered name in the CSA database.

3.1.4 Need for Names to be Meaningful

The subject name listed in a certificate shall identify the Subscriber using the Subscriber's legal name as it appears on the DEA Form 223. If this name cannot be used, the name that Federal or local records refer to that person (e.g., POA letter, human resources documents, birth certificate or drivers license) will be used. The CA must describe in its CPS how the DN will always be unique to each Subscriber.

CSOS Subscriber certificates issued by the CSOS CA shall contain the DN of C=US, O=U.S. Government, OU=Department of Justice, OU=DEA, OU=Diversion Control,

OU=E-Commerce, OU=CSOS, OU="State" and will include the common name (CN) of the individual using the certificate and a serial number that is unique to the Subscriber.

3.1.5 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are established by the PMA. These rules are contained in the *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document. These documents may be found http://www.DEAecom.gov.

3.1.6 Uniqueness of Names

The DN shall be unique for each Subscriber. CA's shall enforce name uniqueness within the X.500 namespace that they have been authorized. A CA shall document in its CPS how they shall allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (i.e., if "Joe Smith" leaves a CA's community of Subscribers, and a new "Joe Smith" enters the community of Subscribers, how shall these two individuals be provided unique names).

3.1.7 Name Claim Dispute Resolution Procedure

CAs will document in their CPS the process by which they will resolve name claim disputes, attempting to resolve all such disputes locally. The PMA shall resolve any name collisions brought to its attention that may affect interoperability.

3.1.8 Recognition, Authentication and Role of Trademarks

The CA shall choose certificate subject names issued under this CP. The CA shall not knowingly issue a certificate including a name that a court of authorized jurisdiction has determined infringes the trademark of the rightful owner. A CA is not obligated to research trademarks or resolve trademark disputes. Any CA may refuse to accept a name known to be a trademark of someone else, or deemed inappropriate for use in the certificate.

3.1.9 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request. This may be done by the entity using its private key to sign a value and providing that value to the CA. The CA shall then validate the signature using the party's public key. The DEA PMA may allow other mechanisms that are at least as secure as those cited here, provided the CA has specified the method in their CPS.

In the case where a key is generated directly on the party's hardware or software token, or in a key generator that benignly transfers the key to the party's token, then the party is deemed to be in possession of the private key at the time of generation or transfer.

If the party is not in possession of the token when the key is generated, then the token (e.g., a smart card or a PKCS #12 encoded message) shall be delivered to the subject via an accountable method specified in the CA's CPS and approved by the DEA PMA.

When keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The CA must maintain a record of validation for receipt of the token by the subject.

3.1.10 Authentication of Organization Identity

The DEA Bridge CA's CPS shall include the procedure to be used for authenticating subordinate and cross-certified CAs. These CAs shall not issue certificates to organizations (as opposed to individuals) referencing the OID of this CP.

3.1.11 Authentication of Individual Identity

EPCS and CSOS Subscriber certificates containing the OIDs referenced in this policy shall be issued only to individuals with controlled substance prescribing or ordering authority as previously defined in Section 1 and to CSOS Coordinators holding local registration responsibility.

3.1.11.1 Authentication of EPCS Subscriber Identity

EPCS Subscriber identity shall be established by an in-person appearance before the CA and/or their local RA, or before a person certified by a State or Federal agency as being authorized to confirm identities (such as a notary public). Process documentation and authentication requirements shall be addressed in the CPS and shall include the following:

- A declaration of identity signed by the applicant using a handwritten signature, performed in the presence of the person performing the identity authentication.
- The identity of the person performing the identification proofing;
- A signed declaration by that person that he or she verified the identity of the Subscriber as required in the CP;

- The date and time of the verification; and
- An identifying number from both the ID of the verifier and the ID of the applicant;

Subscribers shall submit the following information/credentials to their EPCS LRA or EPCS CA for identity verification:

- Two copies of identification, one of which must be government-issued photo identification, such as a driver's license or passport.
- A copy of a current DEA Certificate of Registration – either the applicant's or the applicant's employer's.
- A signed Subscriber Agreement stating that the applicant has read and understands the terms of this CP and has agreed to the statement of Subscriber obligations that the CA provided;
- For practitioners seeking a certificate under the registration of an institutional practitioner:
  - A signed Subscriber Agreement from the registrant indicating that the registrant has read and agreed to the statement of registrant obligations that the CA provided.
  - A letter, on the institution's letterhead, certifying that the registrant currently employs the practitioner(s). The letter must include the practitioners' current work mailing address, work telephone number, and work e-mail address (if applicable);

The subordinate or cross-certified CA shall verify the Subscriber's identity by crosschecking application information with relevant information from the CSA database.

3.1.11.2 Authentication of CSOS Coordinator Identity

A separate application process shall be established for the identification of an organization's CSOS Coordinator. The CSOS RA must receive a CSOS Coordinator application in advance of, or concurrently with, the submission of CSOS Subscriber certificate applications. CSOS Coordinators shall submit the following information/credentials to the CSOS RA for identity verification:

- A signed and notarized CSOS Coordinator application obtained from the CSOS Web site at http://www.DEAecom.gov containing the signature of the individual who signed the most recent application for DEA Registration or the

individual authorized to sign the most recent application for DEA Registration authorizing that individual to represent the organization in the capacity of the CSOS Coordinator.

- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport;
- A copy of a current DEA registration certificate (form 223) of the applicant or the most recent application for DEA registration.
- For individuals with POA to sign orders, a copy of the power of attorney form as specified in Code of Federal Regulations (CFR).

3.1.11.3 Authentication of CSOS Subscriber Identity

Authentication of CSOS Subscriber identity is performed by the local organization and requires the identification of a CSOS Coordinator, who serves as the LRA and organizational point of contact for CSOS issues. Subscribers shall submit the following information/credentials to their designated CSOS Coordinator for identity verification:

- A CSOS Certificate application, signed by the applicant, stating that the applicant has read and understands the terms of this CP and has agreed to the statement of Subscriber obligations that the CA provided;
- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport;
- For individuals with POA to sign orders, a copy of the power of attorney form as specified in CFR.
- The CSOS Coordinator shall sign the application and forward the application packet to the CA.

The CA shall validate application information with relevant information from the CSA database supplied by DEA.

3.1.11.4 Authentication of Component Identities

CA personnel, who are not authorized to order and receive CSOS or EPCS Subscriber certificates, may receive special purpose administrative certificates. These certificates shall not contain the EPCS or CSOS OIDs or authorized schedule extension data referenced in this policy and shall be issued only for the purposes of signing electronic files and communications. Management of these special purpose administrative certificates will be described in the CPS. These certificates may not be used for controlled substance orders.

Computing and communications components (routers, firewalls, servers, Web servers, etc.) may be issued special purpose device certificates in order to secure communications with the CA. These certificates shall not contain the EPCS or CSOS OIDs or authorized schedule extension data referenced in this policy. In such cases, each component shall be named as the certificate subject and must have a human sponsor. The PKI sponsor is responsible for providing the following information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name);
- Equipment public keys;
- Equipment authorizations and attributes (if any are to be included in the certificate);
- Contact information to enable the CA or RA to communicate with the sponsor when required.

3.2 Routine Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period. The CA shall notify the Subscriber 45 days prior to the expiration date of the Subscriber's certificate. The EPCS Subscriber or Subscriber's CSOS Coordinator may request that the CA issue a new certificate for a new key pair, provided that the original certificate has not been revoked, the Subscriber name and attributes are unchanged, and the Subscriber is in good standing with the CA, continuing to qualify as a DEA registrant, CSOS POA, or agent of a DEA registrant as defined in Section One. Electronic requests must be digitally signed using the Subscriber's EPCS-issued certificate or the CSOS Coordinator's CSOS-issued certificate and shall be authenticated on the basis of the Subscriber's or Coordinator's digital signature using the private key for a total of two certificate re-keys. The third request shall require Subscribers to establish identity using the initial registration process described in Sections 3.1. and 4. CAs shall ensure that the Subscriber's identity information and public key are properly bound on all digital requests. Changes to a Subscriber's name, prescribing or ordering authority, or affiliation shall result in certificate revocation as specified in Section 4.

CAs must go through the original registration process to obtain a new certificate. That CA shall notify all CAs, RAs, and Subscribers who rely on the CA's certificate that it has been changed. For self-signed ("Root") certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

The DEA Bridge CA key pair and certificate will not exceed the lifetimes stated in this CP. At re-key, the DEA Bridge CA will post the new public key on the website at http://www.DEAecom.gov.

CAs will document their re-key procedures in their CPS.

3.3 Certificate Update

Updating a certificate means creating a new certificate that has a different key and a different serial number, and that it differs in one or more other fields, from the old certificate. CAs must update Subscriber certificates whose characteristics have changed due to changes in name, affiliation, or prescribing or order authority, as indicated in the daily CSA extracts received from DEA. The old certificate must be immediately revoked.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent (as set forth above) in order for an updated certificate with the new name to be issued. The CSOS Coordinator will serve as the certifier for the name change request submitted to the CSOS RA. All changes to affiliation or authorized schedules require crosschecking applicant information with relevant information from the CSA database.

3.4 Re-key after Revocation

In the event of certificate revocation due to key compromise, cessation of operation, or as a result of negative action taken against the Registrant or Subscriber by DEA, issuance of a new certificate shall require that the Subscriber go through the initial registration process as specified in Sections 3.1 and 4.

3.5 Revocation Request

Revocation requests must be authenticated by the CA. Requests to revoke a certificate may be authenticated via manual signature, telephone call-back or by using that certificate's associated private key to digitally sign the request, regardless of whether the private key has been compromised and must be described in the CPS. Revocation request procedures are described in Section 4.4.4.

Section 4 — Operational Requirements

4.1 Certificate Application

4.1.1 EPCS CA

Requests by EPCS subordinate or cross-certified CAs for CA certificates shall be submitted to the PMA accompanied by a Certificate Policy (if cross-certifying), Certification Practices Statement, a certificate request, and all required supporting documentation. Complete application package information can be found on DEA's Web site at http://www.DEAecom.gov. The submitted CPS shall be written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC2527]* and shall define how the CA shall comply with the DEA Diversion Control E-Commerce System CP. The PMA shall evaluate the CPS for acceptability prior to approving and processing the CA's certificate request.

4.1.2 Subscriber

Eligible Subscribers are those who hold a valid DEA registration as defined in Title 21 CFR Part 1300. All Subscriber applicants shall submit a completed Subscriber application (obtained from their EPCS or CSOS CA) in accordance with Section 3.1.11, entering into an initial agreement with the CA. Upon successful completion of the Subscriber identification and authentication process in accordance with this CP, the applicant shall generate a key pair and demonstrate to the CA that it is a functioning key pair as defined in the CPS.

CSOS Subscribers may obtain Certificate application forms and instructions from http://www.DEAecom.gov. The applicant will follow the procedures in the Subscriber Manual posted on the CSOS web site at http://www.DEAecom.gov, mailing completed applications to the Drug Enforcement Administration, E-Commerce Program (ODC), CSOS Enrollment, Washington, DC 20537. Using the information provided with the application, and verification against the CSA database, the CSOS RA either approves or denies the application. The CSOS RA will notify the Registrant and the Registrant's CSOS Coordinator when the application is received via email when the application is received. Should the application be denied, the CSOS RA will provide notification of the application denial to the applicant and the applicant's CSOS Coordinator.

EPCS CAs will provide application processing information in their CPS.

4.2 Certificate Issuance

4.2.1 Delivery of Public Key for Certificate Issuance

Public keys must be delivered for certificate issuance in a way that binds the entity's verified identification to their public key. In all cases, the method used for public key delivery shall be set forth in the CPS. If cryptography is used, it must be at least as strong as that employed in certificate issuance. This binding may be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request.

4.2.2 Subordinate CAs

Upon approval of a subscribing subordinate CA's CPS, the DEA Bridge CA shall process the certificate request and return a public key certificate. The subscribing subordinate CA must demonstrate the ability to generate valid Subscriber certificates by issuing a test certificate to the DEA Bridge CA. The test certificate must be revoked immediately after generation.

Hardware tokens containing subordinate CA private signature keys may be backed-up in accordance with security audit requirements defined Section 4.5.1.

4.2.3 Cross-Certified CAs

The DEA Diversion Control-E-Commerce System Bridge CA, serving as the authorized DEA Bridge, shall issue a unilateral cross certificate to approved cross-certified CAs. Upon receiving a certificate request from an approved CA, the DEA Bridge CA shall sign and issue a cross-certificate to the entity CA, using a secure non-electronic means. The cross-certified CA must demonstrate the ability to generate valid EPCS Subscriber certificates by issuing a test certificate to the DEA Bridge CA, which shall be revoked immediately after generation.

4.2.4 Subscriber

Upon receipt of a Subscriber's application for certificate, the CA shall confirm the Subscriber's identity against the CSA database extract supplied by DEA. The CA must ensure that this extract content is protected from unauthorized modification. To the extent practical, certificates, once created, shall be checked to ensure that all certificate fields and extensions are properly populated with the data obtained from the CSA database extract. This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

Upon completion of the certificate application process, the CA shall issue the requested Subscriber certificate and notify the applicant in accordance with procedures specified in its CPS. The CA shall make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or made available for pickup by, the approved certificate applicant only. All Subscribers shall generate their own private keys, and shall not require delivery of their private keys.

4.3 Certificate Acceptance

By accepting an EPCS or CSOS certificate, the Subscriber or CA acknowledges that all information contained in the certificate is accurate and reaffirms that he or she agrees to the terms and conditions contained in this CP definition and the applicable Subscriber Agreement.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation of Subscriber Certificates

A certificate shall be revoked when the binding between the Subscriber and the Subscriber's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- An audit indicating that an EPCS CA has violated stipulations of this CP, or its CPS (i.e. if the CA's certificate is revoked, all certificates that it has issued are revoked). CSOS certificates will not be revoked, however suspension of new certificates may be directed by the PMA until audit discrepancies are resolved;

- It can be demonstrated that the Subscriber has violated the stipulations of the Subscriber Agreement;

- Identifying information or affiliation components of any names in the certificate become invalid;

- Privilege attributes (prescribing or ordering authority) asserted in the Subscriber's certificate are reduced;

- DEA posts notice that certificate holder's DEA Registration has been revoked, suspended or restricted, that the Registration information has changed, or that the Registration has been terminated;

- The private key is lost, compromise is suspected, or cannot be accessed for any reason; or

- The Subscriber, the DEA Registrant under whose Registration a certificate holder obtained a certificate, or CSOS Coordinator requests that the affiliated Subscriber certificate be revoked;

CAs who issue EPCS or CSOS Subscriber certificates are required to validate Subscribers against the daily CSA extract provided from DEA. Certificate revocations must be immediately performed for those Subscribers whom have had identifying information, affiliation components, or prescribing or ordering authority reductions as discussed above. CAs must describe their process for validating existing Subscribers against the daily CSA database extract in their CPS.

4.4.2 Circumstances for Revocation of Subordinate CA Certificates

Circumstances under which a subordinate CA certificate or cross-certificate to an approved DEA CA can be revoked include: 1) upon the direction of the DEA Diversion Control E-Commerce System PMA, 2) upon an authenticated request by a previously designated authorized official of the CA's organization (such officials must be designated in the MOA between DEA and the organization or outlined in the organization's CPS), or 3) when the DEA Diversion Control E-Commerce System PMA determine that an emergency has occurred that may impact the integrity of the certificates issued by the DEA Diversion Control E-Commerce System.

In the event that the CA ceases operations, any certificate issued to the CA, and all certificates issued by the CA, must be revoked prior to the date that the CA ceases operations.

4.4.3 Who Can Request Revocation

An EPCS CA certificate may be revoked upon the direction of the PMA or upon the authenticated request of the designated official of the CA.

A Subscriber, the PMA, or other DEA-approved entity may request revocation of the Subscriber's certificate at any time for any reason. A Registrant may request revocation of the certificate of its agent at any time, for any reason. The issuing CA may also revoke a Subscriber's certificate upon the failure of the Subscriber (or the Sponsor, where applicable) to meet its obligations under this CP or any other agreement, regulation, or law applicable to the certificate that may be in force.

4.4.4 Procedure for Revocation Request

A certificate revocation request shall identify the certificate to be revoked and provide the reason for its revocation. If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the revocation request must so indicate.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. All revocation requests shall be authenticated as described in the CA's CPS. Electronic requests may be authenticated using the digital signature of the requestor.

4.4.4.1 CA Certificate Revocation

Revocation of a CA's certificate shall take effect upon the publication of status information in the ARL. Upon revocation, the Bridge CA shall immediately generate and publish status information in the ARL identifying the certificate being revoked and the reason for its revocation. A CA certificate that is revoked shall remain on the ARL until the certificate expires.

4.4.4.2 Subscriber Certificate Revocation

Revocation of Subscriber certificates shall take effect upon the publication of status information identifying the reason for the revocation within the time limits specified in Section 4.4.10.

A Subscriber shall, upon ceasing its relationship with an organization that sponsored the certificate, prior to departure, or upon revocation of a certificate associated with a hardware cryptographic token, surrender to that organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

If a Subscriber leaves an organization and the hardware tokens cannot be obtained from the Subscriber, then all Subscriber certificates associated with the unretrieved tokens shall be immediately revoked. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

4.4.4.2.1 CSOS Subscriber Certificates

Relying Parties are permitted under Title 21 CFR 1305.09 to fill received orders for 60 days after the execution of the order by the purchaser, provided the order was valid at the time of signing. In order to ensure that a revoked certificate that has expired within this 60-day time frame is not accepted, the CA shall continue to maintain Subscriber certificate revocation information on its CRL for a minimum period of **60 days beyond** certificate expiration.

4.4.4.2.2 EPCS Subscriber Certificates

Due to the time limits with which pharmacies are permitted under Title 21CFR 1306.22 to fill or refill received prescriptions for Schedules III or IV controlled substances, provided the order was valid at the time of signing, the EPCS CA shall continue to maintain Subscriber certificate revocation information on its CRLs for a minimum period of **6 months beyond** certificate expiration.

4.4.5 Revocation Request Grace Period

The Subscriber must immediately notify their CSOS Coordinator and CSOS RA when a key compromise is detected, suspected, or when discovered risk is determined to warrant revocation.

The CA shall publish in its CPS the maximum time within which it shall process revocation requests for this and other reasons.

4.4.6 Circumstances for Suspension

Certificate suspension is allowable under the following conditions:

- As a result of a discrepancy reported in compliance audit of a subordinate or cross-certified CA, the PMA may choose to suspend rather than revoke the CA's certificate until the discrepancy has been corrected.
- Subscriber certificates may be suspended if the status of the Subscriber has changed and the PMA deems it appropriate to suspend rather than revoke the Subscriber certificate.

4.4.7 Who Can Request Suspension

Only the PMA, CSOS RA or other DEA-authorized entity may request certificate suspension under the circumstances discussed in Section 4.4.6

4.4.8 Procedure for Suspension Request

The DEA PMA may request the suspension, rather than revocation, of a Subscriber's certificate at their discretion. CSOS Subscriber certificate suspension requests will be made to the DEA Diversion Control E-Commerce System Help Desk via the DEA Diversion Control E-Commerce Section Chief or Operations Manager.

Suspension requests to EPCS-approved CAs will be made from the DEA Diversion Control E-Commerce System Help Desk and must be authenticated. Each EPCS-approved CA shall include suspension authentication request procedures in their CPS.

Certificate suspension will be supported by including the suspended certificate in the CA's ARL or CRL. The CRL shall use the CRLReason code specified as 'certificateHold'.

4.4.9 Limits on Suspension Period

The suspended certificate shall remain on the CA's ARL or CRL until the PMA makes the request through the DEA E-Commerce System Help Desk that the certificate should no longer be suspended. Requests to remove a certificate from suspension must be authenticated. Each EPCS-approved CA shall include these authentication procedures in their CPS.

4.4.10 ARL/CRL Issuance Frequency

ARLs and CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. EPCS and CSOS CAs shall publish a complete CRL every 24 hours or sooner, even if there are no changes to be made. The DEA Bridge CA shall publish a complete Authority Revocation List (ARL) every 30 days or sooner, even if there are no changes to be made. In the event of key compromise, CRLs/ARLs containing the newly revoked certificate information shall be published within 6 hours of notification. In the event of CA certificate revocation, the DEA Diversion Control E-Commerce System shall notify all other CAs via a digitally signed email.

Superseded certificate status information shall be removed from the repository system upon posting of the latest certificate status information, with the latest CRL overwriting the expired CRL.

4.4.11 ARL/CRL Checking Requirements

Relying parties must validate every EPCS and CSOS certificate received in connection with a transaction against a valid and unexpired CRL as required by applicable federal and state regulations. Certificates shall include pointers to CRLs identified in the certificate's cRLDistributionPoints extension field. CRLs and ARLs may be cached and relied upon until they expire, unless otherwise notified by the PMA. In the event that the DEA Bridge CA or CSOS CA is unable to publish its revocation list as described in this CP, the Help Desk will provide notification to all affected EPCS CAs and CSOS Coordinators using either email or a phone call. CSOS Coordinators must perform a

callback to the Help Desk to authenticate the message. This notification will also be posted to the DEA web site at www.deadiversion.usdoj.gov, accessible to all Relying Parties. Notification via email or telephone call will also be provided by the Help Desk to CSOS Coordinators when CRL service has been restored after an interruption of greater than 24 hours.

4.4.12 Checking Requirements for Other Forms of Revocation Advertisements

Practice Note: CAs may use OCSP to distribute status information instead of ARL/CRL provided other terms are met.

4.5 CA Security Audit Procedures

For audit purposes, the CA shall log operational events pertaining to Subscriber enrollment and certificate management. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. The specific procedures for auditing the system shall be stated in the CPS.

4.5.1 Types of Events Recorded

The CA shall record the events identified in the National Institute of Standards and Technology (NIST)-developed Certificate Issuing and Management (CIMC) Protection Profile for Level 3 components. All security auditing capabilities of CA operating system and PKI CA applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- Type of entry;
- The date and time the event occurred;
- A success or failure indicator when executing the CA's signing process;
- A success or failure indicator when performing certificate revocation; and
- Identity of the entity and/or operator that caused the event.

A message from any source requesting an action by the CA is an auditable event; the message must include the message date and time, source, destination, and contents.

Procedures specifying integrity controls, event record lifetime and event record access shall be implemented and maintained. The audit log should be reviewed for abnormalities in support of any suspected violation and for events such as repeated failed actions, requests for privileged information, attempted access of system files, and certificate and revocation requests that fail authentication and validation criteria. A review of event entries must be performed regularly and follow up actions must be taken for suspicious events or omissions.

4.5.2 Frequency of Processing Log

Each CA shall establish procedures within its CPS for the daily review of audit log files wherein a statistically significant set of security audit data generated by the CA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. All significant and notable events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs that might indicate potential compromise. Actions taken as a result of these reviews shall be documented.

CAs shall make audit log summaries available to the PMA for review upon request.

4.5.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. At the end of this period, the security audit log information shall be moved to a safe, secure storage location separate from the CA equipment and shall be retained as archive records in accordance with Section 4.6.

The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.

4.5.4 Protection of Audit Log

CA system configuration and procedures must be implemented together to ensure that only authorized persons read, archive or delete security audit data. The entity performing security audit data archive shall not have modify access. Procedures must be implemented to protect archived data from disclosure, deletion, modification or destruction prior to the end of the security audit data retention period. CA systems must be configured so that audit logs are not overwritten if the log becomes full.

4.5.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. Adequate backup procedures must be in place to comply with archive requirements identified in Section 4.6 and to recover audit log data in the event of a system failure. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

4.5.6 Audit Collection System (Internal vs. External)

The audit log collection system may be internal or external to the CA system. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the CA shall cease operation except for revocation processing until the security audit capability can be restored.

4.5.7 Notification to Event-Causing Subject

No Stipulation.

4.5.8 Vulnerability Assessments

Vulnerability assessments must be routinely conducted and performed prior to initial production or after any configuration changes to identify potential vulnerabilities or events that would affect the integrity and operation of the CA. The CA and other operating personnel shall be watchful for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel.

4.6 CA Records Archival

4.6.1 Types of Events Recorded

CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

- CA accreditation (if applicable);
- Certificate Policy;
- Certification Practice Statement;

- WebTrust for CA accreditation;
- Contractual obligations;
- System and equipment configuration;
- Modifications and updates to system or configuration;
- All certificates issued or published;
- Record of Re-key;
- Certificate requests;
- Revocation requests;
- Subscriber Identity Authentication data as per Section 3.1;
- Documentation of receipt and acceptance of certificates;
- Documentation of receipt of tokens;
- All certificates issued or published;
- Record of Entity CA Re-key;
- All ARLs and CRLs issued and/or published;
- All audit logs and computer security audit data (in accordance with Section 4.5);
- Other data or applications to verify archive contents;
- Documentation required by compliance auditors.

4.6.2 Retention Period for Archive

Archival of the recorded events in Section 4.6.1 shall be retained and protected against modification or destruction for a period specified in the CPS, at least ten years six months. All security audit logs, both electronic and non-electronic, shall be made available during compliance audits. Applications required for processing the archive data shall also be maintained for the same period as the archival records.

Subordinate or cross-certified CAs must submit an electronic archive of all posted EPCS CRLs to the PMA annually.

4.6.3 Protection of Archive

The media that the archive is stored on must be protected at a level required to maintain and protect Subscriber information from disclosure, modification or destruction either by physical security alone, or a combination of physical security and cryptographic protection. It should also be adequately protected from environmental threats such as temperature, humidity and magnetism. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, a Federal agency may retain data using procedures that have been approved by the U.S. National Archives and Records Administration (NARA) for that category of documents.

The contents of the archive shall not be released except as determined by the DEA Diversion Control E-Commerce System PMA or as required by law. Records of individual transactions may be released upon authenticated request of any Subscribers involved in the transaction or their legally recognized agents.

4.6.4 Archive Backup Procedures

CA backup procedures must be in place and shall be sufficiently detailed to establish the proper operation of the CA, or validity of any certificate (including those revoked or expired) issued by the CA.

4.6.5 Requirements for Time-Stamping of Records

No Stipulation.

4.6.6 Archive Collection System (Internal or External)

No Stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store CA archives shall be published in the CA's CPS. Only authorized personnel shall be permitted to access the archive.

4.7 Key Changeover

CA keys shall be changed while sufficient life remains on the certificate to allow uninterrupted validity of all Subscribers. If keys must be changed due to changes in software or hardware, the current keys shall be maintained for a sufficient period to allow uninterrupted validity of all subordinate subjects. New keys shall be generated as per Section 3.2.

4.8 Compromise and Disaster Recovery

4.8.1 Disaster Recovery

The CA shall have in place an appropriate disaster recovery/business resumption plan that is capable of resuming services in accordance with this CP. If CA equipment is damaged or rendered inoperative, but CA signature keys are not destroyed, CA operations shall be reestablished, giving priority to the ability to generate certificate status information, such that ARL/CRLs can be posted within 24 hours of the event. The CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. The CA shall address long-term interruption restoration procedures in its CPS and Contingency Plan.

Recovery/resumption plans must be in place for all potential scenarios (e.g. inadvertent destruction/corruption of critical systems/data, natural disaster, and terrorism) recognized in a current risk assessment. The CA must identify redundant capabilities (e.g. back-up systems, location of archived data, records/key availability, and off-site facilities/personnel). A list of key personnel and their contact information must be easily accessible in the event of an emergency.

4.8.2 Key Compromise Plan

The CA must have in place an appropriate key compromise plan that defines the procedures that shall be followed in the event of a compromise of the private signing key used by the CA to issue certificates. Such a plan shall include procedures to revoke all affected CA, and EPCS and CSOS Subscriber certificates and procedures that allow for the prompt notification of all Subscribers and known relying parties. The plan shall also include procedures for the prompt re-issuance of valid certificates.

4.9 CA Termination

In the event that the DEA Bridge CA terminates operations, the PMA shall notify all subordinate CAs and cross-certified CAs, who shall then, in turn, notify all Subscribers and known relying parties of the termination prior to the termination date.

In the event that a subordinate or cross-certified CA terminates operations, the CA shall notify the PMA, all Subscribers, and known relying parties of its upcoming termination prior to the termination. All certificates issued by the CA that reference this CP shall be revoked no later than the time of termination.

Section 5 — Physical, Procedural, and Personnel Security Controls

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The location and construction of the facility housing CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

The CA equipment shall always be protected from unauthorized access, and especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. At a minimum, the physical access controls should:

- Ensure that no unauthorized access to the hardware is permitted;
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers;
- Be manually or electronically monitored for unauthorized intrusion at all times;
- Ensure an access log is maintained and inspected periodically;
- Require two-person physical access control to both the cryptographic module and computer system.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules and CA equipment shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the CA equipment shall occur if the facility is to be left unattended for an extended period of time. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed"; and for the CA, that all equipment other than the repository is shut down);
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

Each CA, and all associated RAs, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing authorized CA services. Proper physical barriers shall be in place. For instance, surrounding walls shall extend from real ceiling to real floor not raised floor to suspended ceiling. The facility shall be locked and intruder detection systems shall be activated while the facility is unoccupied and tested periodically. Fire prevention and protection controls shall be in place including a fire extinguisher system. CA facilities must be constructed so as to prevent exposure of systems to water.

The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed which are not parts of the CA operation. The CA's facility shall also store backup and distribution media in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information.

5.1.3 Physical Access Controls

Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the equipment environment. The CA facility's main entrance shall be attended during normal working

hours. The main entrance shall be controlled by electronic access control devices during non-working hours. Physical access to the CA's systems must be limited to authorized individuals with a valid purpose to enter. Authentication controls must be used to access areas containing the CA's systems. Visible identification shall be worn while in the area of the CA's systems. Those persons not authorized to enter the facility but who require access for business purposes, can enter the facility, only if an authorized manager or member of the operations staff escorts them. Their arrival and departure must be recorded. Visitors working unsupervised in the area of the CA's systems are prohibited. All access to the facility must be logged.

CA equipment shall always be protected from unauthorized access. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

The CA is required to:

- Ensure that no unauthorized access to the CA is permitted;
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers;
- The facility shall manually or electronically monitor for unauthorized access and intrusion at all times;
- Ensure an access log is maintained and inspected daily.

A security check of the facility housing the CA equipment shall occur prior to leaving the facility unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation;
- Security containers are properly secured;
- Physical security systems are functioning properly;
- The area is secured against unauthorized access.

An access policy detailing the procedures for physical access shall be maintained and reviewed periodically. A person, or group of persons, shall be made explicitly responsible for making physical security checks. When a group of persons is responsible for making physical security checks, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall sign a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.4 Power and Air Conditioning

The CA facility shall be supplied with power and air conditioning sufficient to create a reliable operating environment and to automatically lockout additional input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Personnel areas within the facility shall be supplied with sufficient utilities to satisfy operational, health, and safety needs.

5.1.5 Cabling and Network Devices

Cabling and network devices supporting CA services shall be protected from interception and damage.

5.1.6 Media Storage, Handling, Destruction and Reuse

CA storage media and devices containing storage media shall be inspected to ascertain if they contain sensitive data prior to disposal or reuse. Items found to contain sensitive information must be physically destroyed or securely overwritten at least three times, using a disk formatting utility designed especially for the permanent removal of data from media, prior to reuse. Items whose contents cannot be determined must be physically destroyed. Storage media used by the CA shall be protected from environmental threats of temperature, humidity and magnetism.

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

5.1.7 Off-site backup

Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an offsite location (separate CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the CA.

Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CAs.

5.1.8 Physical Security Controls for End Entities

A Subscriber shall physically protect any password or PIN that allows entry into the Subscriber's digital certificate. Passwords or PINs should be memorized and not written down. If a password or PIN needs to be written down, it shall be stored in a locked file cabinet or container accessible only to designated personnel.

At no time shall Subscribers leave their system unattended while the cryptographic module, or private key, is activated.

5.2 CA Procedural Controls

The CA's operating procedures must be documented and maintained to provide guidelines for secure and accurate operation of the facility. Accurate procedures detailing roles, responsibilities, and tasks must exist to control setup, changes and use of equipment, software and operating procedures. Reporting and response procedures must exist detailing points of contact and actions to be taken in the event of security incidents and malfunctions.

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. To ensure that one person acting alone cannot circumvent safeguards, CA responsibilities and authority shall be divided between multiple roles and individuals.

The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. The primary trusted roles defined in this policy can be directly mapped to the FBCA and CIMC Protection Profile developed by NIST as follows: CA Operator (maps to the Administrator role), RA Operator (maps to the Officer role), Security Officer (maps to the Auditor role), and System Administrator (maps to the Operator role). While DEA-approved CAs may have different name designations for these roles, it is expected that the separation and distribution of functions shall be consistent with this policy and shall be employed at all CA and RA locations.

5.2.1.1 Shareholders

The Shareholder role serves to ensure multi-person control of sensitive CA information by safeguarding hardware that is essential to the creation of the CA keys. As such, Shareholders do not hold an account on any of the systems. Shareholders are required to

participate in any task that requires authentication to or activation of the CA's private signing key.

5.2.1.2 CA Operator (Administrator)

The CA Operator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

CA Operators shall have no part in Subscriber certificate adjudication and adequate controls shall be in place to prevent the CA Operator from issuing unauthorized Subscriber certificates.

5.2.1.3 RA Operator (Officer)

The RA Operator's role and corresponding procedures shall be defined in the CPS. The officer role is responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the certificate issuance process;
- Requesting, approving and executing the certificate revocation process.

5.2.1.4 Security Officer (Auditor)

The Security Officer's role is responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the FBCA or Entity CA is operating in accordance with its CPS;

5.2.1.5 System Administrator (Operator)

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.6 Other Trusted Roles

The CA shall list other relevant trusted roles and their responsibility not specifically cited in this CP.

5.2.2 Separation of Roles

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the RA Operator (Officer), CA Operator (Administrator), Security Officer (Auditor) roles, or System Administrator (Operator) role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both a CA Operator (Administrator) and RA Operator (Officer) role, assume both the CA Operator (Administrator) and Security Officer (Auditor) roles, or assume both the Security Officer (Auditor) and RA Operator (Officer) role. No individual shall be assigned more than one identity.

5.2.3 Identification and Authentication for Each Role

Individuals shall identify and authenticate themselves before being permitted to perform any actions involved in a trusted role. User access shall be initiated and terminated through a registration procedure. Accounts and passwords shall be issued and managed in a manner ensuring the integrity of the system. User rights and privileges must be limited to the duties and responsibilities of the individual to which they are issued. Users access rights shall be reviewed regularly. Policies regarding password length, complexity, and use shall be strictly adhered to.

5.3 Personnel Controls

Each CA and its associated RA shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this CP.

All personnel involved in DEA Bridge or subordinate CA functions shall be properly trained to ensure that all functions as stipulated by this CP are competently performed.

5.3.1 Personnel Security Controls for Certification Authorities

The CA shall identify at least one individual or group responsible and accountable for the operation of the CA. The individual assuming the role of CA Operator should exhibit unquestionable loyalty, trustworthiness, and integrity, and should demonstrate a high degree of security consciousness and awareness in their daily activities. All persons

filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens.

All CA personnel shall:

- Not be assigned other duties that would interfere with their regular duties and responsibilities;
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Be appointed in writing by an approving authority;
- Have received proper training in the performance of their duties.

5.3.2 Clearance Procedures

It is the position of DEA that the conviction of crimes and unauthorized use of controlled substances are activities that are proper subjects for inquiry during personnel background investigations in order to fairly assess the likelihood of an employee committing a drug security breach. Therefore, employee-screening procedures must include the following questions of the employee:

1) Within the past five years, have you been convicted of a felony, or within the past two years, of any misdemeanor or are you presently formally charged with committing a criminal offense? (Do not include any traffic violations, juvenile offenses or military convictions, except by general court-martial.) If the answer is yes, furnish details of conviction, offense, location, date and sentence.
2) In the past three years, have you ever knowingly used any controlled substances, other than those prescribed to you by a physician? If the answer is yes, furnish details.

Background checks are required for personnel filling positions where a high degree of trust is required and shall demonstrate that the requirements set forth in Section 5.3.1 and this section are met. These background checks should be compliant with applicable fair employment practices and employee privacy rights and must include inquiries of courts and law enforcement agencies for past and pending charges or convictions. These procedures are an ongoing process and must be reviewed periodically. Background check procedures shall be described in a CA's CPS.

5.3.3 Training

CA employees must receive training in the organizational policies, CA/RA security principles and mechanisms, all PKI software versions in use on the CA system, all PKI

duties they are expected to perform, and disaster recovery and business continuity procedures. Training must be an ongoing and documented process. Any significant change to CA operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Documentation shall be maintained identifying all personnel who received training and the type of training completed.

Personnel performing duties with respect to the operation of a CA shall receive:

- Training in the operation of the software and/or hardware used in the CA system;
- Training in the duties they are expected to perform;
- Briefing on stipulations of the CA's CPS and this CP;
- Ongoing training in security procedures and policies.

5.3.4 Sanctions for Unauthorized Actions

The CAs, OMA or PMA may suspend an individual's access to the CA system if that individual has performed actions involving the CA not authorized in this CP or the CA's CPS.

Breach of this CP or the CPS whether through negligence or with malicious intent, is subject to privilege revocation, administrative discipline, and/or criminal prosecution.

5.3.5 Employee Termination Controls

Once an employee holding a position of trust or any level of system access leaves the organization, their physical access and system access must be revoked upon receipt of termination documentation to ensure system integrity.

5.3.6 Contracting Personnel

Contractor personnel acting as representatives of DEA, employed to operate any part of the DEA Bridge CA and CSOS CA, are subject to the same background checks as U.S. Government personnel, and shall be cleared to the level of the role performed.

5.3.7 Documentation Supplied to Personnel

This CP and relevant parts of the CPS shall be made available to the CA and associated RA personnel. Operation manuals shall be made available to CA personnel to facilitate the operation and maintenance of the CA.

5.3.8 Personnel Security Controls for End Entities

In addition to the CP, Subscribers shall be provided with information on the use and protection of the software used within the EPCS and CSOS domains. The CA shall provide a technical help desk support for all Subscribers.

Section 6 — Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The DEA Bridge CA and subordinate or cross-certified CAs shall generate cryptographic keying materials using FIPS 140-1 level 3 or 140-2 level 3 validated cryptographic modules. The CA's key pair must be generated on a token in such a way that use of the private key at all times remains in control of authorized user(s) of the key pair.

Subscribers' signature key material for certificates issued by the CAs shall, at a minimum, be generated using a FIPS 140-1 level 1 or 140-2 level 1 validated cryptographic module.

6.1.2 Private Key Delivery to Entity

Private keys shall not be transferred or exchanged. All entities shall generate their own private keys, and shall not require delivery.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber's public key must be transferred to the RA or CA in a way that ensures:

- It has not been altered during transit;
- The sender possesses the private key that corresponds to the transferred public key;
- The sender of the public key is the legitimate user claimed in the certificate application.

6.1.4 CA Public Key Delivery to Users

The public key of the CA signing key pair may be delivered to end entities in an online transaction in accordance with IETF PKIX Part 3, PKCS 7 or via another appropriate trustworthy mechanism as defined in the CA's CPS. The CA shall post the certificate it issues in the CA repository or CA Web site.

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below:

The DEA Bridge CA and subordinate or cross-certified CA signature keys must be FIPS 186-2 approved of at least 2048 bits (standard) for RSA or DSA, and at least 283 (elliptical) bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use Secure Hash Algorithm version 1 (SHA-1) in accordance with FIPS 186-2. Signatures on certificates and CRLs that are issued after 1/1/09 shall be generated using SHA-256.

Subscriber keys that expire before 12/31/08 must be at least 1024 bit RSA with a FIPS 186-2 approved hashing function. Subscriber keys that expire on or after 12/31/08 shall contain public keys that are at least 2048 bit RSA, in accordance with FIPS 186-2.

Use by the CA of SSL, TLS, or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/08. Use of SSL, TLS, or another protocol providing similar security to accomplish any of the requirements of this CP shall require, at a minimum, AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/08.

6.1.6 Public Key Parameters Generation

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-2.

6.1.7 Parameter Quality Checking

Parameter quality checking (including testing for prime numbers) shall be performed in accordance with FIPS 186-2.

6.1.8 Hardware/Software Key Generation

The DEA Bridge CA and subordinate or cross-certified CA key generation shall be performed solely in hardware. At a minimum, the generation process for the DEA Bridge and subordinate CAs shall be FIPS 140-1 Level 3 or, 140-2 Level 3, compliant.

At a minimum, the generation process for Subscribers shall be FIPS 140-1 Level 1 or 140-2 Level 1 compliant and shall be generated in the client's system.

EPCS Subscriber keys shall be stored on a token device under the sole control of the Subscriber.

6.1.9 Key Usage Purposes (as per X.509 v3 key usage field)

CA and Subscriber signing keys must only be used for digital signature and non-repudiation; CA signing keys may also be used for certificate and CRL signing as specified in the *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document.

6.2 Private Key Protection

The CA and Subscriber must take adequate steps to protect their private keys in accordance with this CP.

CSOS Subscriber keys may be generated in software or hardware and must remain under the sole control of the Subscriber. CSOS Subscriber keys shall not be escrowed or backed-up.

6.2.1 Standards for Cryptographic Module

At a minimum, DEA Bridge and subordinate or cross-certified CA cryptographic modules must be validated to the latest version of FIPS 140 series - Level 3 (hardware).

At a minimum, CSOS Subscriber cryptographic modules must be validated to the latest version of FIPS 140 series - Level 1 (hardware or software).

At a minimum, EPCS Subscriber cryptographic modules must be validated to the latest version of FIPS 140 series - Level 2 (hardware).

6.2.2 Private Key (n out of m) Multi-Person Control

A minimum of two persons shall be required for all CA operations activities.

6.2.3 Private Key Escrow

Under no circumstances shall a key used to support non-repudiation services be escrowed by a third party.

6.2.4 Private Key Backup

CA private signature keys shall be backed up under the same multi-person control as the original signature key. Such backup shall create only a single copy of the signature key at the CA location; a second copy may be kept at the CA backup location. All copies of the backed-up key must be handled in an accountable manner that protects against unauthorized access and unauthorized use. Procedures to affect this shall be included in the CPS.

Backup of the Subscriber's private key is prohibited.

6.2.5 Private Key Archival

Subscriber private signature keys shall not be archived, escrowed, or copied. See Sections 6.2.3 and 6.2.4.

6.2.6 Private Key Entry into Cryptographic Module

The CA signing private key pair shall be generated and handled by cryptographic modules in a manner compliant with FIPS 140-1 level 3 or 140-2 level 3.

6.2.7 Method of Activating Private Key

Authorized personnel shall log on to the CA systems to activate CA private signing keys in accordance with Section 5.2.2. The means of authentication shall be dual-factor and

shall be described in the CPS. Acceptable means of authentication include, but are not limited to, pass-phrases, PINS or biometrics (fingerprint, iris or retinal scan, facial or voice recognition). Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

CSOS Subscribers must be authenticated to the cryptographic module before the activation of any private key(s). Approved means of authentication include pass-phrases, PINs or biometrics (fingerprint, iris or retinal scan, facial or voice recognition).

EPCS Subscribers must be authenticated to the cryptographic module by means of biometric authentication (fingerprint, iris or retinal scan, facial or voice recognition, or other NIST-approved biometric technology) before the activation of any private key(s).

For all Subscribers, entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.8 Method of Deactivating Private Key

After use, the CA cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Subscriber cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated (e.g., via a manual logout procedure, or automatically after a period of inactivity). Hardware cryptographic modules shall be maintained under the control of the Subscriber.

6.2.9 Method of Destroying Private Key

The specific mechanism for destroying CA private keys shall be defined in the CPS and must be approved by the PMA.

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA public key shall be archived in accordance to the procedures described in Section Four.

6.3.2 Usage Periods for the Public and Private Keys

The usage period for a CA key pair is a maximum of six years. CA private keys may be used to generate certificates for the first half of the usage period (3 years), and the public key may be used to validate certificates for the entire usage period. If the CA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period. Subscriber certificates shall expire upon the expiration of the Subscriber's DEA registration. Subscribers must renew their CSOS and EPCS certificates to continue to conduct CSOS or EPCS business electronically.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data (password) used to unlock the CA or the Subscriber's private key, in conjunction with any other access control, shall be generated in conformance with FIPS-112 and shall result in a high level of strength for the keys or data to be protected. CAs shall document their rules on password selection in their CPS.

Subscriber activation data must be user selected and be generated in conformance with FIPS-112. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Activation data used to unlock the CA or Subscriber private key shall be securely protected against modification and disclosure by a combination of cryptographic and physical access control mechanisms. Activation data for private keys associated with certificates asserting individual identities shall never be shared. The protection mechanisms for CAs shall be described in their CPS.

Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module. If activation data is written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

The CA activation data protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the CPS.

6.5 Computer Security Controls

The computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards and must be outlined in a CA Security Plan.

The operating system shall enforce the identification, authentication, auditing, and separation of roles of all users. A secure logon process shall be used to access the CA's systems. An access control policy and an account management process shall be implemented to restrict access to information and system functions. Isolation of sensitive systems to a dedicated computing environment is required. The system must employ an inactivity time-out period of no greater than ten minutes after which the certificate holder must re-authenticate to access the private key. Malicious software detection and prevention controls must be implemented and must be kept current. This is an ongoing task. Procedures must exist to address prevention, removal, recovery, and documentation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The CA shall use software that has been designed and developed under a formal, documented development methodology. Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase). Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf (COTS) hardware or software.

All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location.

New equipment and software, including patches and updates, must be thoroughly tested on a separate platform for functionality and vulnerabilities prior to being implemented on operational systems. Operational systems must be physically and logically separate from developmental systems and systems used for testing software patches and updates to maintain integrity of services provided. Risks must be examined as a part of the configuration management process and vulnerability assessments must be conducted on operational systems after the installation of software patches, updates, or modifications that result in significant changes to configuration settings. Procedures for implementation on operational systems shall be developed during testing on isolated systems.

Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. All hardware and software shall be scanned for malicious code on first use and periodically thereafter.

6.6.2 Security Management Controls

A security document must exist that details security controls that have been implemented to the system. This document must provide guidance for the secure operation of the CA and for ensuring the integrity of its operating environment. Responsible individuals shall implement and maintain the security policy.

The configuration of the CA and supporting systems, as well as any modifications and upgrades shall be documented and controlled through formal change management processes. There shall be a mechanism for detecting unauthorized modification to CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the CA system. The CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.7 Network Security Controls

CAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Access to unused ports and services must be denied to prevent misuse. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. Users shall be provided access only to services that they are specifically authorized to use from terminals designated for that function. Connections to services from network paths other than those

specified for that function must be refused. Dial-up or external access to the CA via system administration interface is prohibited. External threats shall be mitigated by controls such as firewalls, network intrusion detection systems and router access lists to protect the internal network. Any network software present on the CA equipment shall be necessary to the functioning of the CA. The CA shall document security attributes of all network services.

6.8 Cryptographic Module Engineering Controls

Requirements for cryptographic modules are as stated in Section 6.1.

Section 7 — Certificate and CRL Profiles

The *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document provides guidance on certificate and CRL profiles, and is published as a separate document. The information in this section of the CP provides only a subset of the data included in the *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document.

All certificates issued by the DEA Bridge CA and its subordinate or cross-certified CAs shall conform to the *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document established by the PMA.

7.1 Certificate Profile

The CA certificate shall be issued in the X.509 format, and shall include a reference to the OID for this CP within the Certificate Policies field. Supported certificate extensions shall be identified in the CPS. CAs must issue Subscriber certificates as specified within the *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document established by the DEA.

7.1.1 Version Number

The DEA Bridge and subordinate or cross-certified CAs shall issue X.509 version 3 certificates.

7.1.2 Certificate Extensions

Certificate extensions used by authorized participants shall conform to the *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document established by the DEA.

7.1.3 Algorithm Object Identifiers

At a minimum, one of the following algorithms must be used and/or supported by CAs and End-Entities for signing and verification:

Algorithm	Object Identifier	Issuing Authority
sha1WithRSAEncryption	1 2 840 113549 1 1 5	RSADSI
DSA-with-SHA1	1 2 840 10040 4 3	X9-57
ECDSA with SHA-1	1 2 840 10045 1	ANSI-X9-62

7.1.4 Name Forms

Every DN must be in the form of an X.501 printable string. In a certificate, the issuer DN and subject DN fields shall contain the full X.500 Distinguished Name of the CA.

7.1.5 Name Constraints

Subject and Issuer DNs must comply with DEA Diversion Control E-Commerce System standards and be present in all certificates.

7.1.6 Certificate Policy Object Identifier

CAs must ensure that the appropriate DEA Diversion Control E-Commerce System CP OID is contained within the Subscriber and subordinate or cross-certified CA certificates.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

CSOS Subscriber certificates must have the policyQualifier extension populated with an explicit text notice as follows:

> This is a DEA CSOS Digital Certificate. It is specifically intended for use in signing controlled substance orders - any other signing uses are at the discretion of the certificate holder.

EPCS Subscriber certificates must have the policyQualifier extension populated with an explicit text notice as follows:

> This is a DEA EPCS Digital Certificate. It is specifically intended for use in signing controlled substance prescriptions - any other signing uses are at the discretion of the certificate holder.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

CAs issuing certificates under this CP shall mark the CP extension as non-critical. Critical extensions shall be interpreted as defined in IETF RFC 3280.

7.2 CRL Profile

7.2.1 Version Number(s)

The DEA PKI Bridge CA shall issue X.509 version 2 CRLs in accordance with the *DEA Diversion Control E-Commerce System Certificate and CRL Profile* document.

7.2.2 CRL and CRL Entry Extensions

All Entity PKI software must correctly process all ARL/CRL extensions identified in the *DEA Diversion Control E-Commerce System Certificate and CRL Profile*. ARLs/CRLs shall be issued in a format that is consistent with the [FPKI-PROF].

Section 8 — Specification Administration

8.1 Specification Change Procedures

The PMA shall review this CP at least once every year. Errors, updates, or changes to this CP shall be communicated to subordinate and cross-certified CAs. All policy changes under consideration by the PMA shall be disseminated to interested parties. All interested parties shall provide their comments to the PMA in a fashion to be prescribed by the PMA.

8.2 Publication and Notification Policies

Only editorial changes or typographical corrections may be made to this specification without notification. Any item in this CP may be changed with 90 days notice. Changes to items, which shall not materially impact a substantial majority of the CAs or relying parties using this CP, may be changed with 30 days notice.

Thirty days prior to major changes to this CP, a notification of the upcoming changes shall be posted and conveyed to subordinate or cross-certified CA organizations.

8.3 CPS Approval Procedures

The PMA shall make the determination that a CPS complies with this policy.

Section 9 — Glossary

Access Control	Process of granting access to information only to authorized users, programs, processes, or other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The Subscriber is sometimes also called an "applicant" **after** applying to a CA for a certificate, but before the certificate issuance procedure is completed.
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Authority Revocation List (ARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being such as a fingerprint.

Certificate	A digital representation of identity. Subscriber certificates identify the individual named in the certificate, bind that person to a particular public/private key pair, and provide sufficient information demonstrating the Subscriber is operating under the authority of the DEA Diversion Control E-Commerce System program.
Certificate Policy (CP)	A "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [X.509]. The DEA Diversion Control E-Commerce System Certificate Policy specifies (1) the Certification Authorities, the Subscribers, and the Relying Parties authorized to participate in the PKI program described by this Policy, (2) the obligations of the participants governed by this Certificate Policy, and (3) the minimum requirements for the issuance and management of digital certificates used within the EPCS and CSOS programs - and other suitable applications.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates that it has issued that are revoked prior to their stated expiration date.
Certification Authority (CA)	A generic term in the context of this CP that applies to an entity authorized by the DEA to issue CSOS or EPCS certificates. Approved. This term is used in this CP to sometimes refer to the DEA Bridge CA, as well as the subordinate CAs or cross-certified CAs that would be operated by DEA or other entities in compliance with DEA regulations.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate Re-key	The act or process of extending the validity of the certificate by issuing a new certificate with a new key pair.
Certification Practices Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific CP requirements.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cross-Certified CA	A Certification Authority that has been issued a certificate by the DEA Bridge CA that establishes a trust relationship between the CA and DEA Bridge CA in order that it may issue EPCS Subscriber certificates.
Cryptographic Module	Set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
CSOS	Controlled Substances Ordering System. A secure electronic system for the transmission of controlled substances orders without the supporting paper DEA Form 222.
Drug Enforcement Administration (DEA)	The DEA regulates the manufacture and distribution of controlled substances in the United States.
DEA Bridge CA	A term assigned to DEA's "Root" Certification Authority that issues other CA certificates. The DEA Diversion Control E-Commerce System Bridge CA serves as a Root CA to the CSOS CA and other DEA-approved CAs participating as subordinate CAs in EPCS, while serving as a Bridge CA to those DEA-approved CAs that are issued certificates allowing cross-certification.
End Entity	Relying Parties and Subscribers.
EPCS	Electronic Prescriptions for Controlled Substances. A secure electronic system for the transmission of prescriptions for controlled substances.
Federal Information Processing Standards (FIPS)	These are Federal standards that prescribe specified performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge Property or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Internet Engineering Task Force (IETF)	A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the architecture and the smooth operation of the Internet.
Key Changeover	The procedure used to change CA keys.
Key Escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	An alphanumeric number registered with an internationally recognized standards organization used within PKI to uniquely identify policies and supported cryptographic algorithms.
Operations Management Authority (OMA)	Parties responsible for managing all personnel and activities involved in the day-to-day operations of the Certification Registration Authority and Help Desk.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	CAs that process the registration of Subscribers and operate according to the stipulations of a Certificate Policy.
Relying Party	A Relying Party is the entity that, by using a Subscriber's certificate to verify the integrity of a digitally signed message, identifies the creator of a message, and relies on the validity of the public key bound to the Subscriber's name. The Relying Party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The Relying Party must use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Revoke a certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat shall exploit a particular vulnerability with a particular harmful result.
Root CA	A term assigned to a Certification Authority that issues other CA certificates. The DEA Diversion Control E-Commerce System Bridge CA serves as a "Root CA" to the CSOS CA, while serving as a Bridge CA to those CAs that are issued certificates allowing cross-certifications. The DEA Bridge CA shall operate in accordance with the provisions of its Certification Practices Statement. The DEA Bridge CA shall also perform the following functions: (1) accept and process applications for operations from subordinate CAs; (2) issue certificates to subordinate CAs approved by the PMA; (3) publish subordinate CA certificate status information.

Server	A system entity that provides a service in response to requests from clients.
Subordinate CA	A subordinate CA is a CA authorized by the PMA to create, sign, and issue public key certificates to authorized EPCS and CSOS Subscribers. Subordinate CAs operates in a hierarchical PKI, subordinate to the DEA Bridge CA.
Subscriber	A Subscriber is the entity whose name appears as the subject in a certificate issued by a DEA EPCS or CSOS Subordinate CA, who attests that it uses its key and certificate in accordance with the Certificate Policy asserted in the certificate. EPCS and CSOS Subscribers are limited to DEA registrants and agents of registrants as stipulated in the Code of Federal Regulations (CFR) §1301.22.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Trusted Role	A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.
Vulnerability Assessments	Vulnerability assessments are conducted to identify potential vulnerabilities or events that would affect the integrity and operation of the CA.